REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
2004	Final	09/21/02 – 07/31/04

4. TITLE AND SUBTITLE
Threat Networks and Threatened Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER
N00014-02-1-1033

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
H. Eugene Stanley

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Trustees of Boston University
881 Commonwealth Avenue
Boston, MA 02215

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Naval Research
Ballston Centre Tower One
800 North Quincy Street
Arlington, VA 22217-5660

10. SPONSOR/MONITOR'S ACRONYM(S)
ONR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
none

14. ABSTRACT
See attached

15. SUBJECT TERMS
network, robustness, resilience, flow, disorder

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			H. Eugene Stanley
unclassified	unclassified	unclassified	UL	5	19b. TELEPHONE NUMBER *(include area code)* 617-353-2617

ABSTRACT

[A.]Network robustness.The goal of this work is to determine network design guidelines which maximize the robustness of networks to both random failure and intentional attack while keeping the cost of the network constant. We find optimal parameters for: (i) scale free networks having degree distributions with a single power-law regime, (ii) networks having degree distributions with two power-law regimes, and (iii) networks described by degree distributions containing two peaks.

[B.] Resilience of Networks: An attack on a network is aimed at interrupting the flow of information in the network. The efficiency of the network in transmitting information between two nodes depends on the length of the optimal path of least cost between them. Our previous work had shown that when the loads on the links are distributed over several orders of magnitude, the average optimal path length scales as a power of the network size N. In such a case the network is said to be in the regime of "strong disorder". This situation is detrimental to the efficient flow of information on the network. In our work we focussed on quantifying the point at which the network starts experiencing strong disorder and therefore starts losing its functionality.

[C.] Dynamics of flow in complex netwoks: Understanding flow in complex networks is important if we are to understand how information, disease, resources, etc flow in the real world. In particular it is important to understand the nature of flow in the presence of disorder. Our work has focused on determining if there is a relationship between the scaling of flow variables and the scaling of other previously studied quantities such as the optimal path. Our preliminary finding is that current flow in a random resistor lattice has the same scaling as the optimal path under conditions of both strong and weak disorder.

Threat Networks and Threatened Networks

H. Eugene Stanley
Boston University
590 Commonwealth Avenue
Boston , MA 02215
Phone: 857 891 1941 Fax: 617 353 3783 Email: hes@bu.edu

Award Number: N00014 02 1 1033
Website: **http://polymer.bu.edu/hes**

CONCISE PROGRESS SUMMARY

[A.]Network robustness. Networks with a given degree distribution may be very resilient to one type of failure or attack but not to another. The goal of this work is to determine network design guidelines which maximize the robustness of networks to both random failure and intentional attack while keeping the cost of the network (which we take to be the average number of links per node) constant. We find optimal parameters for: (i) scale free networks having degree distributions with a single power-law regime, (ii) networks having degree distributions with two power-law regimes, and (iii) networks described by degree distributions containing two peaks. Of these various kinds of distributions we find that the optimal network design is one in which all but one of the nodes have the same degree, k1 (close to the average number of links per node), and one node is of very large degree, k2 ~ N^2/3, where N is the number of nodes in the network.

[B.] Resilience of Networks: An attack on a network is aimed at interrupting the flow of information in the network. One way this can be achieved is by overloading the routes (links) in the network. The efficiency of the network in transmitting information between two nodes depends on the length of the path of least cost between them. This path is called the optimal path. Our previous work had shown that when the loads on the links are distributed over several orders of magnitude, the average optimal path length scales as a power of the network size N. In such a case the network is said to be in the regime of "strong disorder". This situation is detrimental to the efficient flow of information on the network. In our recent work we focussed on quantifying the point at which the network starts experiencing strong disorder and therefore starts losing its functionality. Our principal finding is that the "strength" of the disorder required to make optimal paths very long, grows as a power of the network size N.

[C.] Dynamics of flow in complex netwoks: Understanding flow in complex networks is important if we are to understand how information, disease, resources, etc flow in the real world. In particular it is important to understand the nature of flow in the presence of disorder(strong and weak). Studying the dynamics process of flow may help us determine efficient methods to prevent or accelerate flow in different situations. Our work has focused on determining if there is a relationship between the scaling of flow variables and the scaling of other previously studied quantities such as the optimal path. Our preliminary finding is that current flow in a random resistor lattice has the same scaling as the optimal

path under conditions of both strong and weak disorder. This provides insight into the important role of geometric properties such as the optimal path in dynamic processes such as current flow.

LONG-TERM GOALS

- We will improve the mathematical principles that characterize universal classes of networks in order to generate models of real world network dynamics that are capable of evaluating real-world network robustness and stability.

- We will develop principles and algorithms to improve modeling of the topologies of highly complex, real-world networks with large numbers of nodes.

- We will generate new strategies and algorithms to improve the stability and safety of threatened networks.

- We will create design principles for optimal resistance of different types of networks to epidemics, malfunctions and attacks. These principles will also have significant implications for the design of efficient and secure algorithms for organizational data flow.

- We will leverage our past work for effective immunization of networks to create strategies for greatly reducing failure cascades and other spreading hazards in threatened networks (i.e., computer viruses, power grid failures, infectious agents).

OBJECTIVES

Our scientific goal is to uncover mathematical principles for the analysis of network architectures and network dynamics for universal classes of network designs (such as small-world, scale-free, random and hybrid, ``heterogenous" networks found in the real world). These principles will enable scientists to accurately model the behavior of network phenomena relevant to a wide range of real-life social, physical, and spatial networks of interest to military planners. Specific networks of interest include: networked forces, information networks, terrorist networks and physical infrastructure networks such as computer networks and power grids.

APPROACH

This research team will use statistical methods based on new concepts in the network analysis approach from physics, the correlated site-bond percolation theory, to analyze the structure and stability of scale-free networks under conditions of random and intentional attack. This is a novel, multi-disciplinary approach to the problem of network stability and network protection with wide application to social networks, the disruption of covert networks, communications and transportation networks, and protection against bioterror threats.

Our approach will involve extensive computer simulations to determine both static and dynamic properties of various network classes. In addition, we will make use of exact analytical solutions where they can be applied.

WORK COMPLETED

The transition between the two scaling laws followed by the optimal path length in the strong and weak disorder regimes was quantified.

The optimal network design for networks under both random and targeted and random attacks was found.

RESULTS

[A].We find that the most robust network under both random and targeted is one in which all but one of the nodes has degree k1 (close to the average number of links per node), and one node is of very large degree, k2 ~ N^2/3, where N is the number of nodes in the network.

[B.]We quantified the transition of the scaling behavior of the optimal path with network size between the logarithmic regime found in the case where the disorder on the network is weak, and the power law regime found when the disorder is strong. Specifically, for a given implementation of disorder with a continuously variable parameter representing the disorder strength, we found the crossover value of the disorder strength parameter at which the scaling behavior of the optimal path length switches from the logarithmic regime to the power law regime. The result of our study is that the crossover disorder strength grows as a power law with the network size.

[C.] We found that the current flow in a two dimensional lattice with either weak or strong disorder belongs to the same universality class as the optimal path.

IMPACT/APPLICATIONS

This research project will improve modeling of terrorist, infrastructural, and bio-chemical warfare using approaches drawn from social network analysis, graph theoretic approaches, and spatial/physical network approaches supported by other Department of Defense grants. It will assist in the creation of decision tools for defense planners to analyze networks (social, physical, spatial, information and organization) capable of spotting vulnerabilities and assisting in the design of networks for a wide variety of defense uses. This work will have significant impact on ongoing and upcoming projects at the Office of Naval Research and DARPA in addressing asymmetrical threats.

One of the attack strategies to debilitate a network is to severely load the network so that optimal routes of communication become very long. This is the regime of "strong disorder". The result of our work enables us to estimate by studying the distribution of loads on the links, at what point the network is pushed into the realm of strong disorder, and thus rendered inefficient.

Our work on network robustness allows network designers to design networks which have maximum robustness with respect to waves of targeted and random attacks.

TRANSITIONS

NONE

RELATED PROJECTS

No related projects reported.

REFERENCES

- Buchanan, M. (2002). Nexus: small worlds and the groundbreaking theory of networks. W. W. Norton & Company, New York.
- Watts, D. J. (2003). Six degrees: the science of a connected age. W. W. Norton & Company, New York.
- Barabasi, A.-L. (2002). Linked: the new science of networks. Perseus Publishing, Cambridge MA.

PUBLICATIONS

Journal Articles.

- G. Paul, T. Tanizawa, S. Havlin and H. E. Stanley. Optimization of robustness of complex networks. Eur. Phys. J. B, 38, 187-191 (2004) *(peer reviewed)*
- S. Sreenivasan, T. Kalisky, L. Braunstein, S. Buldyrev, S. Havlin, and H. E. Stanley (2004). Effect of disorder strength on optimal paths in complex networks, Phys. Rev. E (accepted for publication)(2004). *(peer reviewed)*
- S. V. Buldyrev, S. Havlin, E, Lopez, and H. E. Stanley, Universality of the optimal path in the strong disorder limit Phys. Rev. E Rapid Communications (accepted for publication) (2004). *(peer reviewed)*
- S. V. Buldyrev, N. V. Dokholyan, S. Erramilli, M. Hong, J. Y. Kim, G. Malescio, and H. E. Stanley,. ``Hierarchy in Social Organization" Physica A ,330, 653-659 (2003). *(peer reviewed)*

ADDITIONAL INFORMATION

HONORS

No honors reported.

STATISTICS

Statistics were not reported.

Print Report | Back